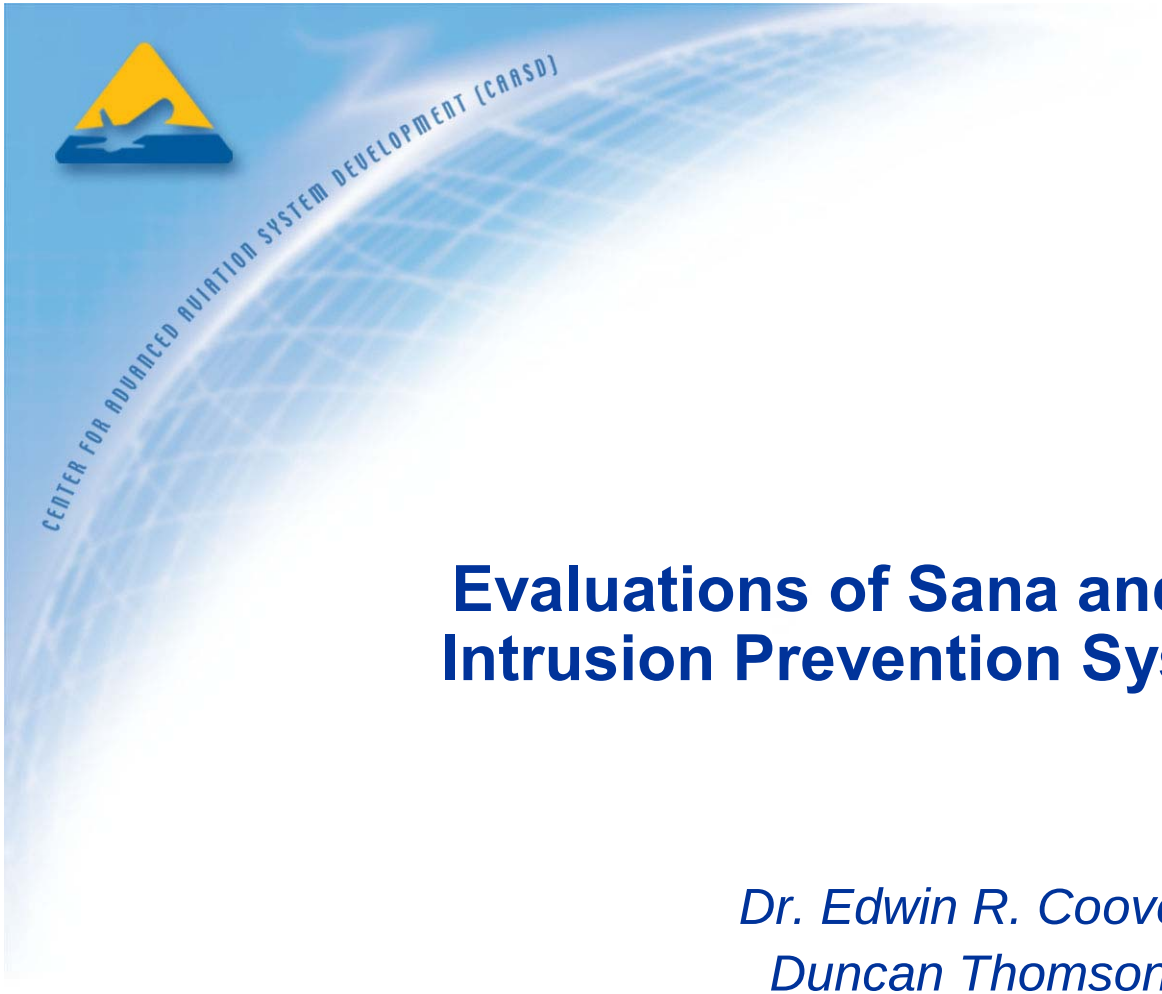


Evaluations of Sana and Cisco Host Intrusion Prevention Systems (HIPS)

Dr. Edwin R. Coover
Duncan Thomson

May 2-5, 2005

CAASD

MITRE

Contents

- Research objective
- The products tested
- The nature of the MITRE testing
- The results of the MITRE tests
- Lessons learned with the testing
- The prospect for ‘adaptive’ products
- MITRE’s recommendations

Research Objective

- Undertaken as part of CAASD's Information Security Systems (ISS) technology research for the Federal Aviation Administration's (FAA) National Airspace System (NAS)
- Work directed by Debra Herrmann (AIO-4)
- Evaluation of Host Intrusion Prevention Systems (HIPS) was one part of a broader investigation in assessing the potential for an "adaptive quarantine," whereby a wide variety of attacks on NAS networks and computers could be identified, isolated and defeated

MITRE

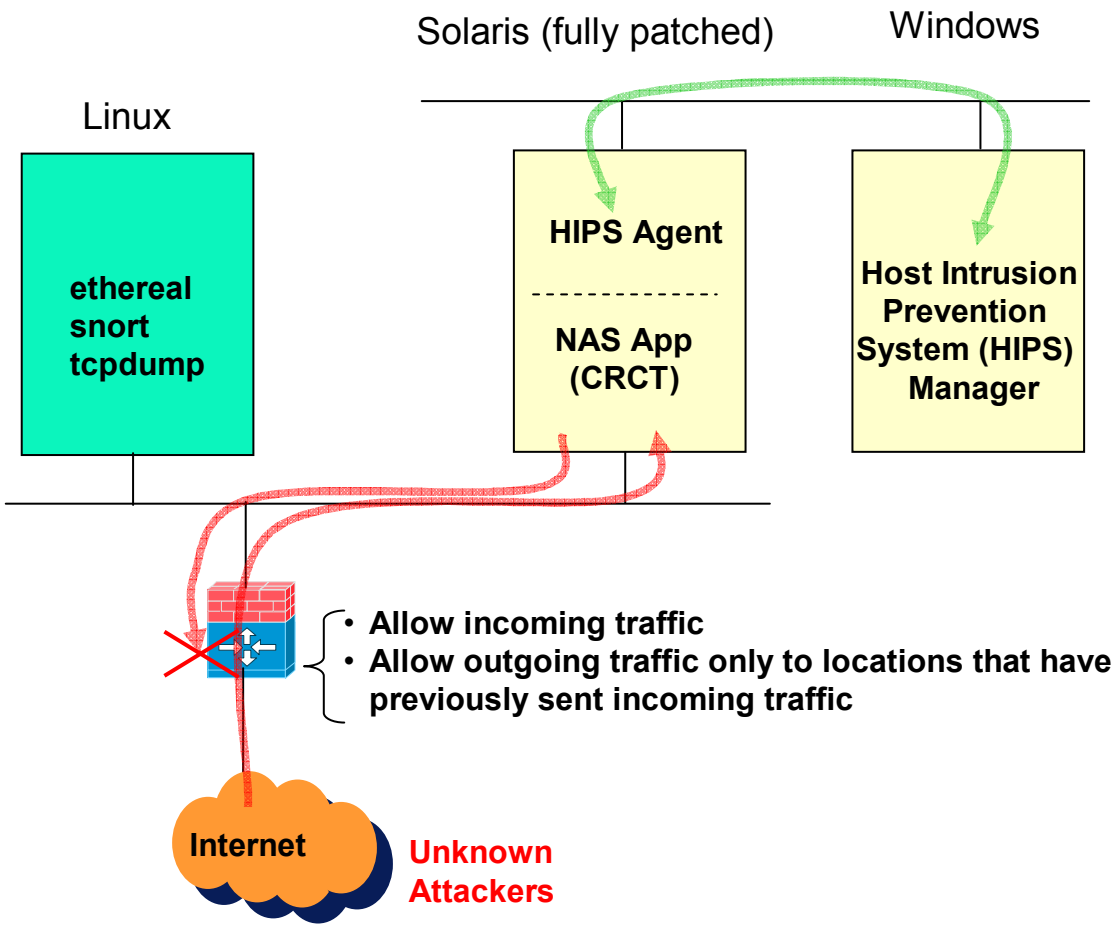
Sana's "Primary Response"

- Anomaly-based HIPS available for Windows and Solaris environments
- Well-documented theoretical basis
- Version tested was Primary Response 2.1
- Test duration was March 29 - April 12, 2004
- Sample configuration (agents for 10 servers, 2 management stations, maintenance) costs $37,500

Cisco's "Cisco Security Agent" (CSA)

- Recent acquisition by Cisco of Okena's "StormWatch" and "StormFront" products
- Rules-based artificial intelligence (AI) HIPS with optional anomaly-based advisor called "Profiler"
- Also available for Windows clients
- Version tested was CSA 4.0
- Test duration was April 6 - 24, 2004
- Sample configuration (agents for 10 servers, 2 management stations, maintenance) costs $33,633 (not including "Profiler")

HIPS Internet-Based Evaluation



MITRE

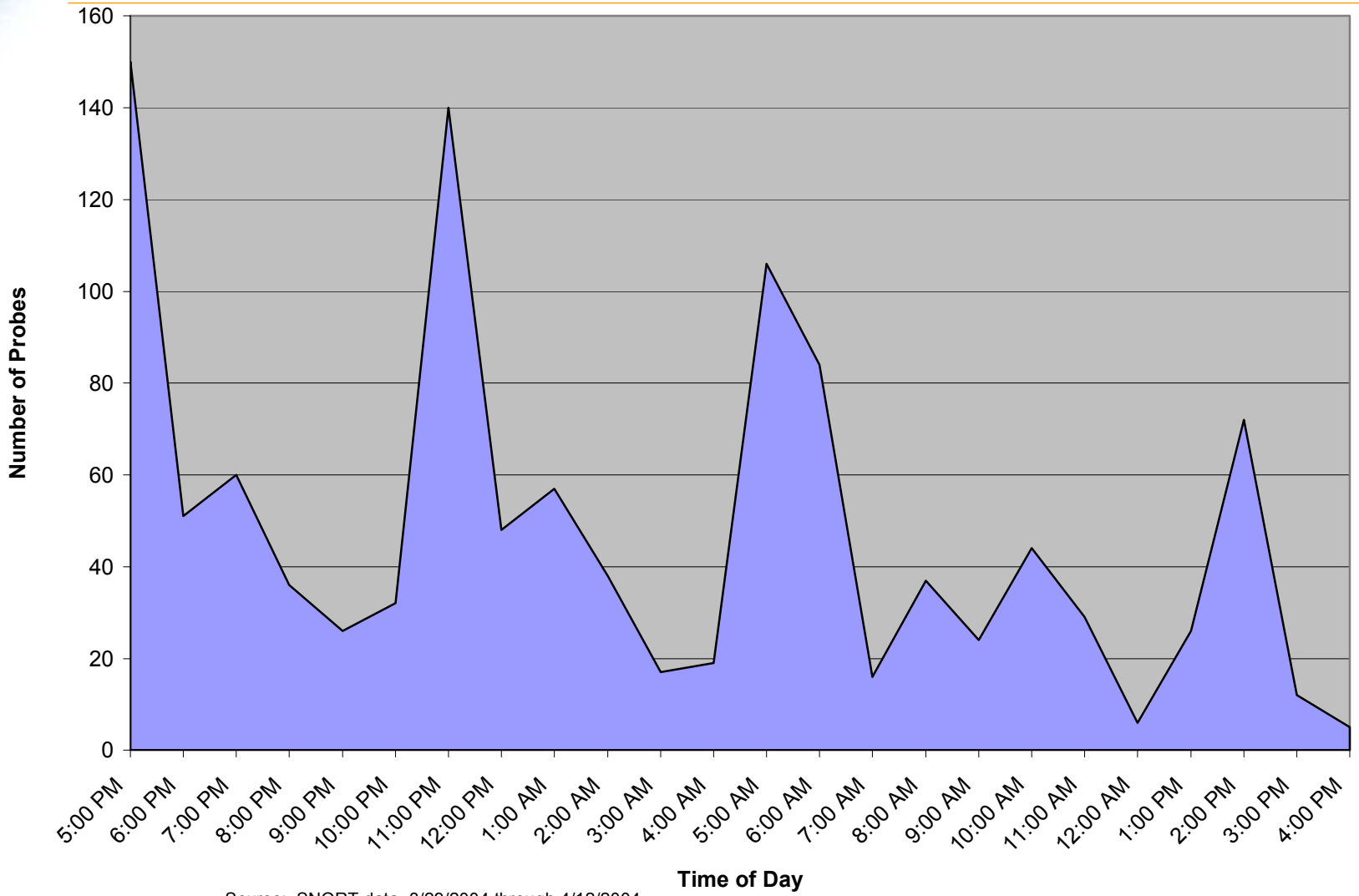
Frequency & IP addresses of probers—Of 1,486 probes received from 658 different IP addresses, the "Top 20" addresses accounted for 70% (462)

Frequency	Source IP Address	Network & Location
62	218.80.52.66	CHINANET Shanghai province
46	61.133.63.113	CNCGROUP Shandong province
42	218.58.78.61	CNCGROUP Shandong province
38	218.88.233.205	CHINANET Sichuan province network
32	67.170.193.197	Comcast Cable Communications IP Services BAYAREA-12
22	220.94.246.85	KORNET-HOTLINE003313798
19	218.76.148.141	CHINANET Hunan province network
18	61.133.71.42	Shandong Cable TV station
17	220.184.235.86	CHINANET-ZJ Hangzhou node network
16	172.129.150.125	AOL-172BLK (Dulles, VA)
16	218.29.35.201	CNCGROUP Henan province network
16	24.130.132.208	CCCH3-30 Comcast Cable Communications Holdings, Inc., Mt. Laurel, NJ
16	65.60.212.145	WIDEOPENWEST OHIO-COL-3-128
16	66.169.148.144	Charter Communications FTWTH-TX-66-169-144
16	67.10.72.128	RR-SOUTHEAST-BLK2 (Herndon, VA)
16	67.172.131.92	Comcast Cable Communications IP Services COLORADO-9
16	68.161.205.75	VIS-68-160 (Verizon Internet Services, Reston, VA)
15	211.38.141.139	KORNET-EXPRESS2003234107
12	218.149.117.134	KORNET-MYIP2003285848
11	218.61.111.240	CNCGROUP Lianoning province network

Source: SNORT data, 3/29/2004 through 4/12/2004, Duncan Thomson, MITRE Corporation.

MITRE

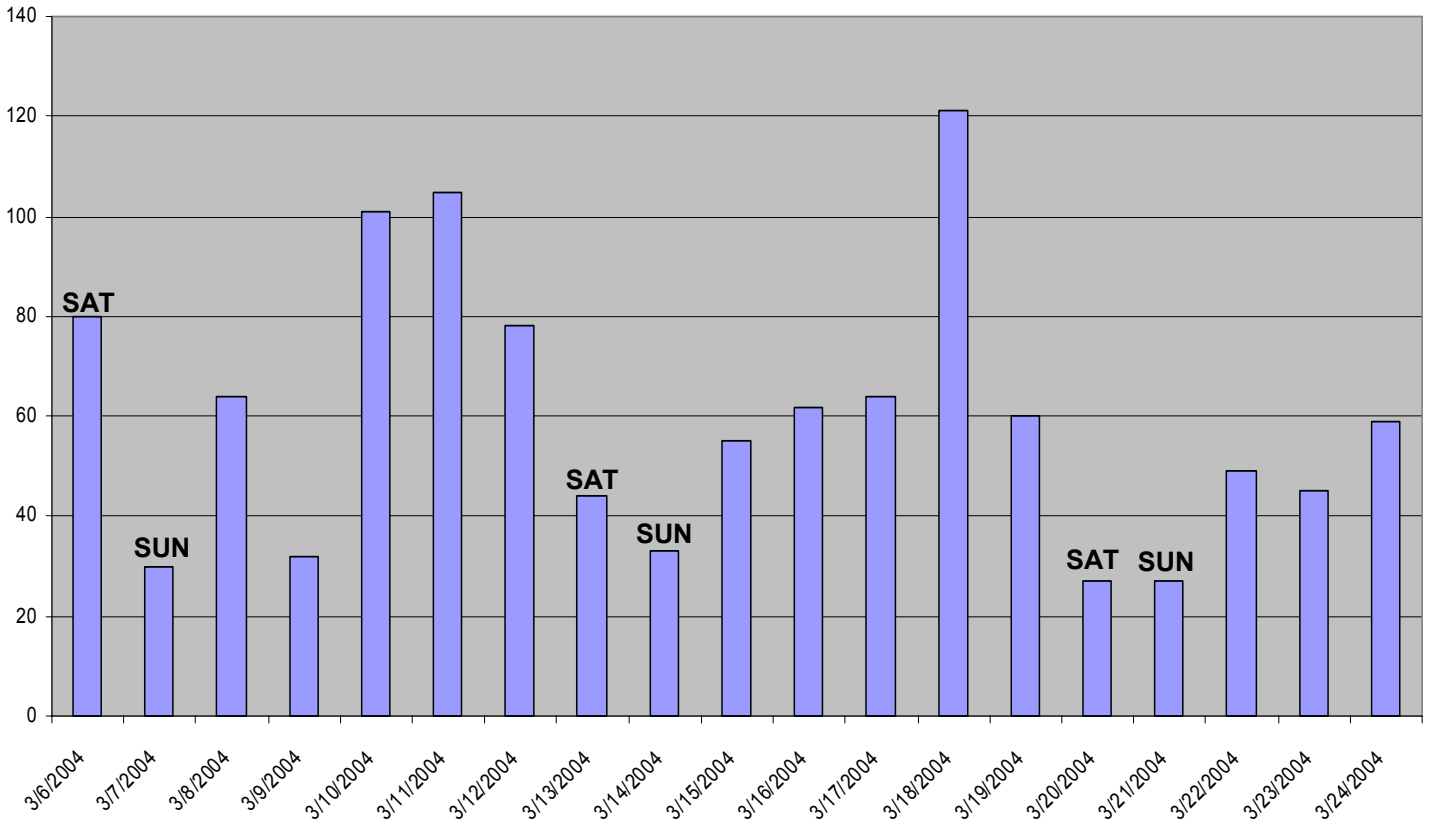
Most of the probes appear to come before or after the normal working day (Eastern Standard Time)



Source: SNORT data, 3/29/2004 through 4/12/2004, Duncan Thomson, MITRE Corporation.

MITRE

The volume of probes over full days in March appears random, but four of the five lowest days (less than 40) are on weekends



Data source: SNORT data by Duncan Thomson, MITRE Corporation, between March 6-24. The sample consisted of 1,136 probes based on 18, 24-hour days, yielding an average of 63 probes per day.

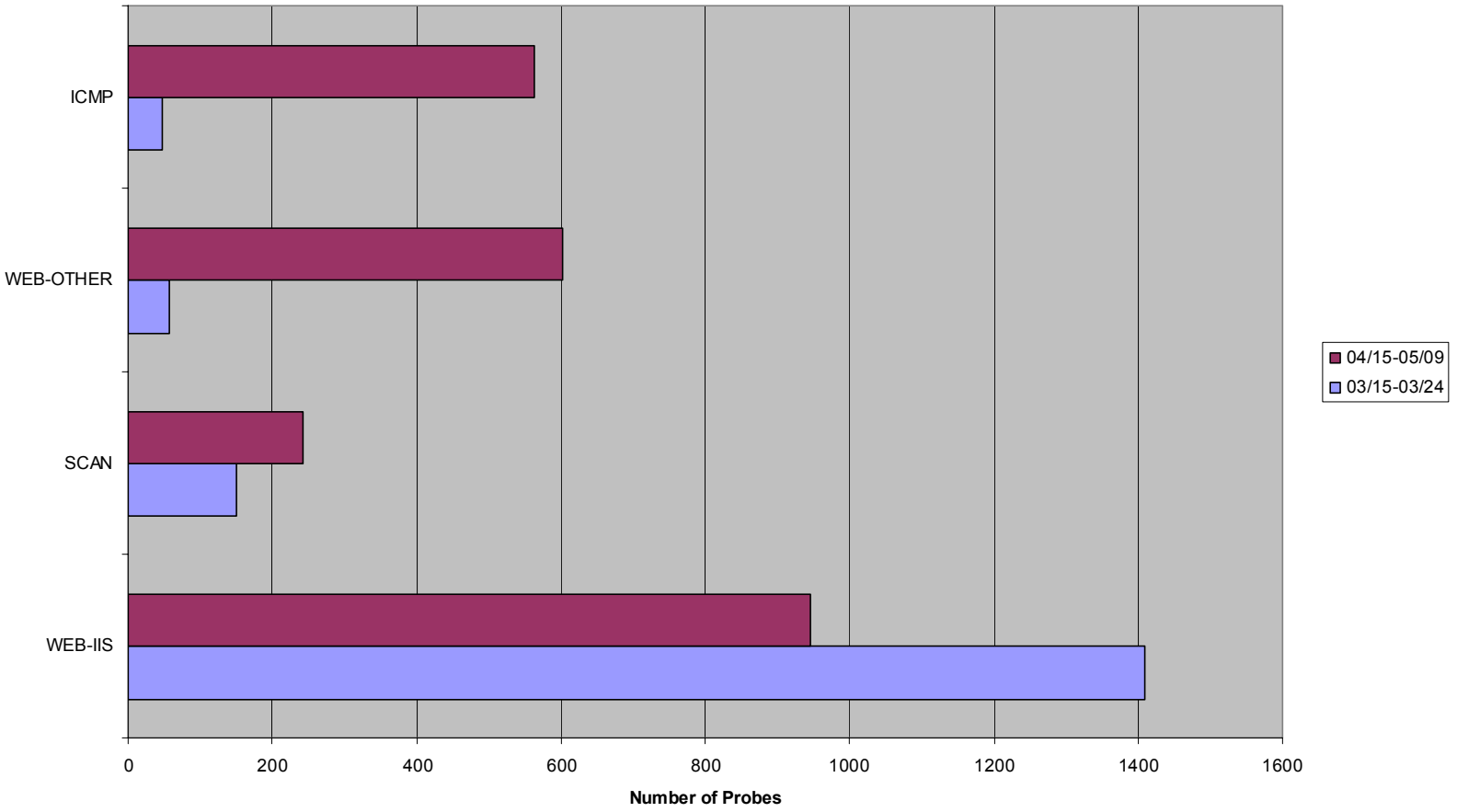
MITRE

Low hanging fruit—50% (740) of all probes were directed at Port 80 and Microsoft's Internet Information Server (IIS)

Number	Types of Exploits Detected By SNORT
1	(spp_stream4) STEALTH ACTIVITY (SYN FIN scan) detection
1	WEB-IIS nsiislog.dll access
2	ICMP redirect host
2	ICMP superscan echo
3	SNMP public access udp
5	SCAN Proxy Port 8080 attempt
7	SCAN SOCKS Proxy attempt
11	WEB-FRONTPAGE /_vti_bin/ access
11	WEB-IIS _mem_bin access
24	WEB-IIS CodeRed v2 root.exe access
25	ICMP Destination Unreachable (Communication Administratively Prohibited)
54	WEB-IIS unicode directory traversal attempt
290	WEB-IIS ISAPI .ida attempt
295	SCAN Squid Proxy attempt
361	WEB-IIS cmd.exe access
395	WEB-MISC WebDAV search access

Source: SNORT data, 3/29/2004 through 4/12/2004, Duncan Thomson, MITRE Corporation.

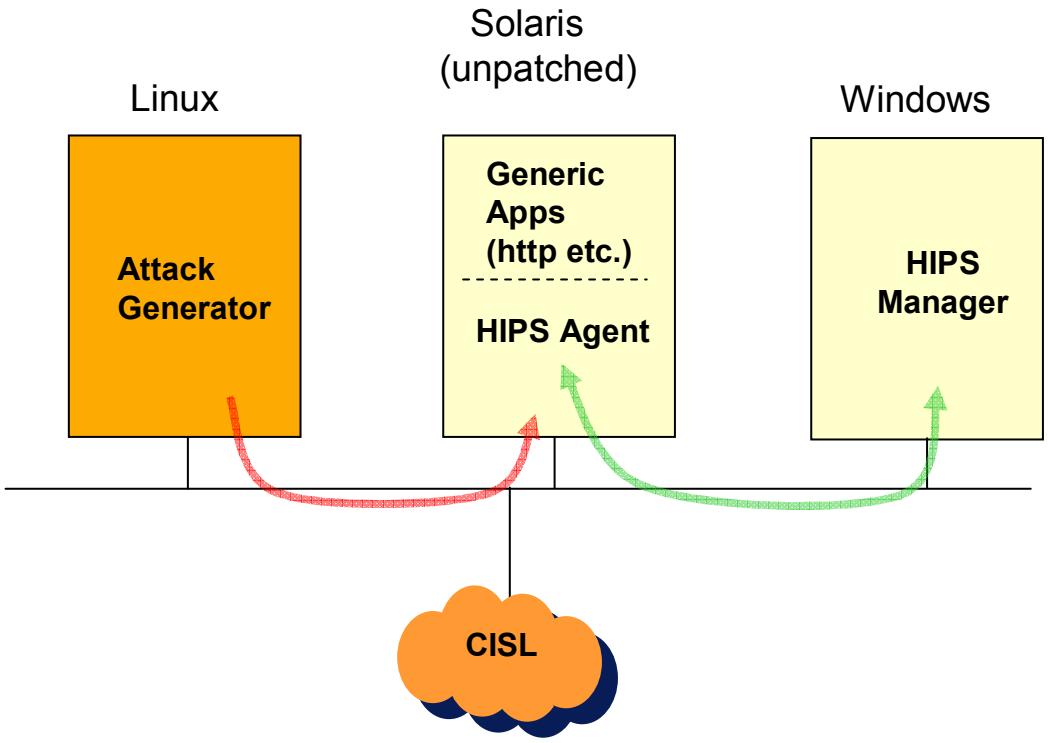
The MITRE CISL presence on the Internet becomes better-known: Probes per full day increased by 32% with the action moving away from WEB-IIS toward the WEB-Other, ICMP and Scans categories



Data source: SNORT data by Duncan Thomson, MITRE Corporation, March-April, 2004. Probe categories with fewer than five cases (15 total) were deleted; the revised combined samples equaled 2,346.

MITRE

HIPS Laboratory-Based Evaluation



MITRE

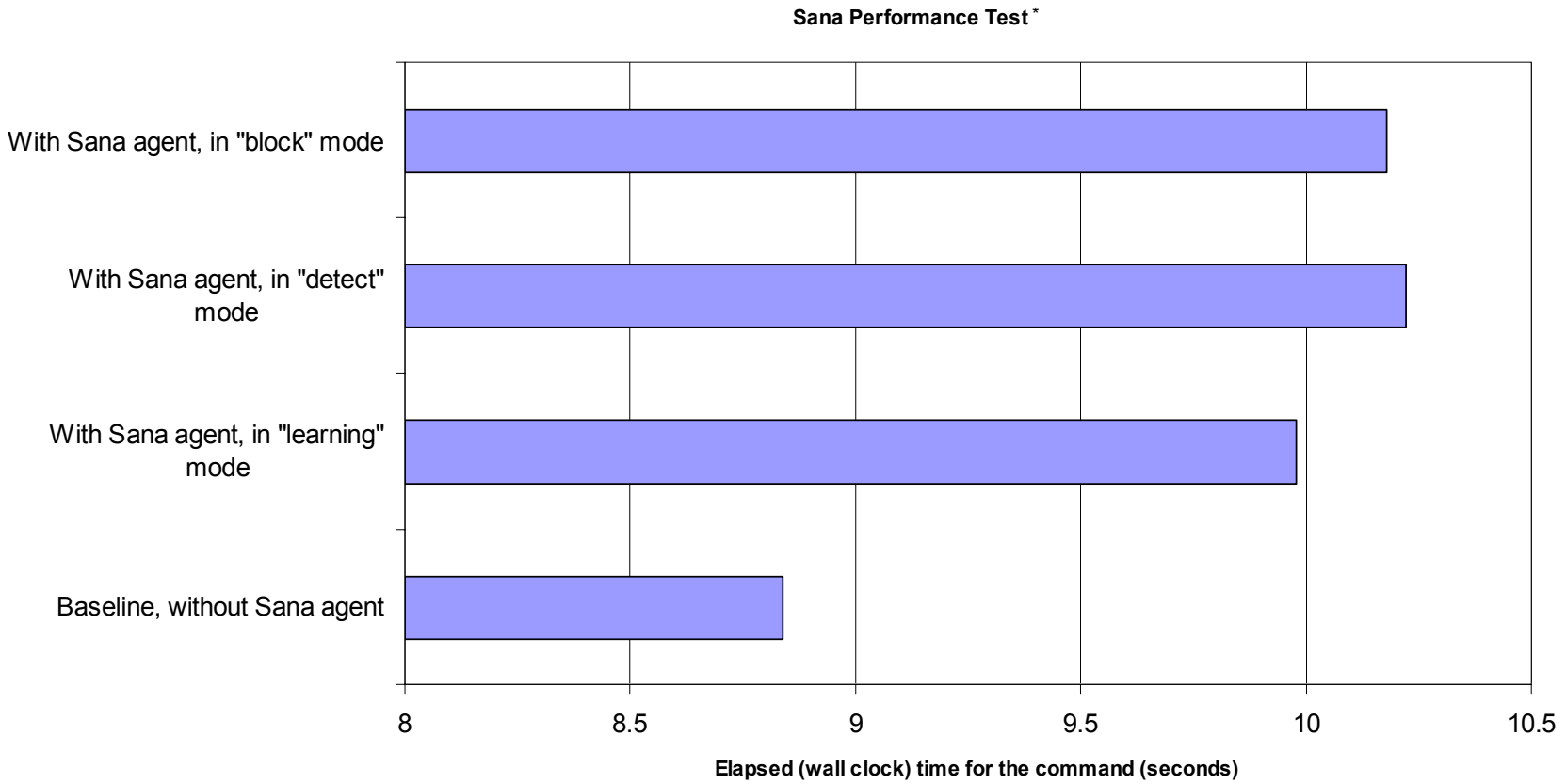
Laboratory Exploit Results

Exploit	Sana Results	Cisco CSA Results
Local buffer overflow code injection (mydateXploit)	Not detected, exploit succeeded*	Exploit blocked, event generated
Remote buffer overflow code injection (snmpXploit)	Not detected, exploit succeeded*	Exploit blocked, event generated, vulnerable daemon killed
Remote “Fail Open” exploit (telnet/rlogin TTYPROMPT exploit)	Not detected, exploit succeeded*	No alert generated, unauthorized login succeeded, however subsequent actions blocked.

* The vendor claims to have made improvements in this area since the CAASD evaluation was conducted.

SANA Primary Response CPU Overhead

Sana HIDS overhead appears to be in the range of 15%

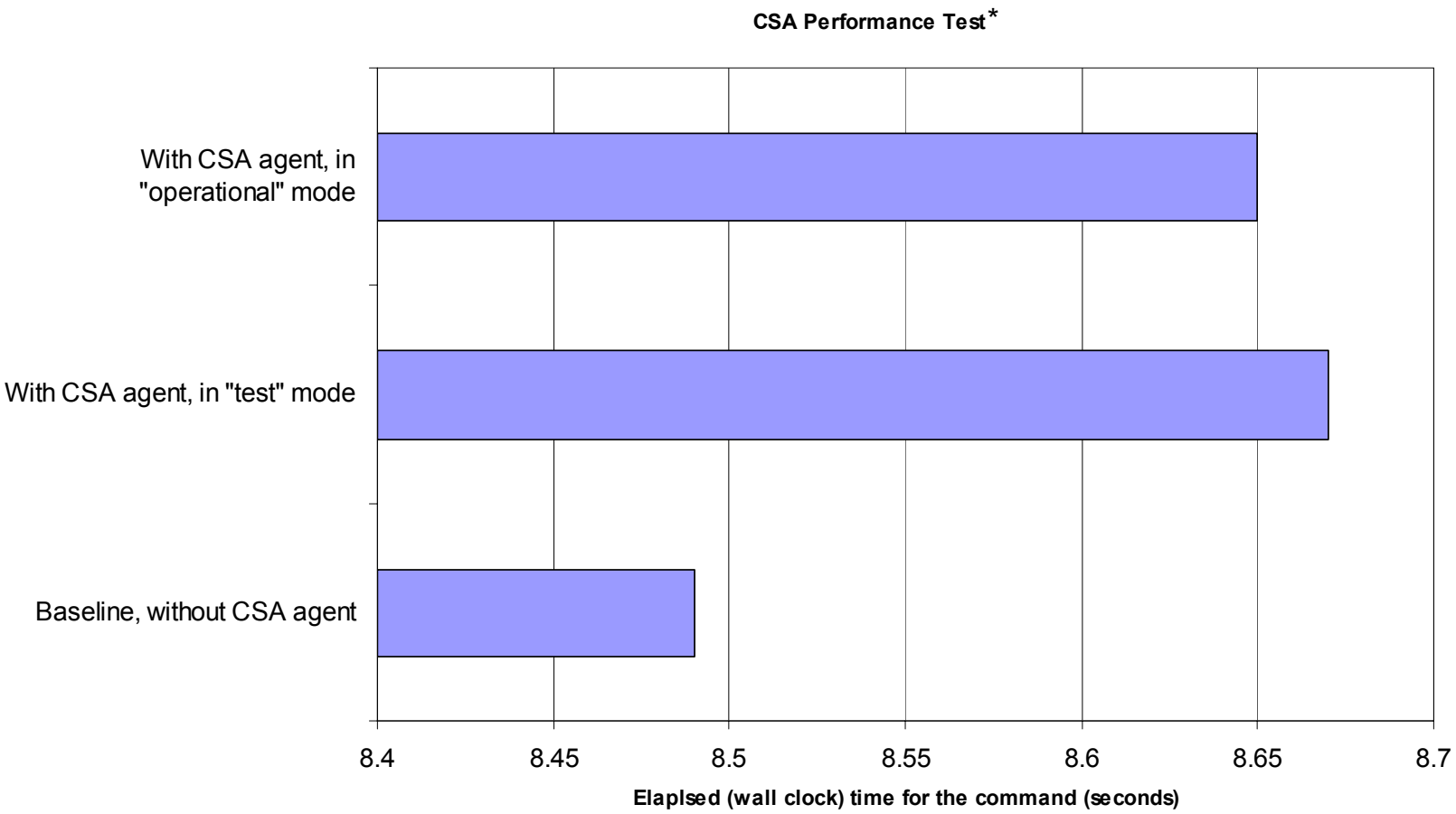


* The performance indicator employed was the time to perform SNMP “MIB Walk” operations. “Block” mode consisted of blocking all unexpected file access and all buffer overflows. Data source: Duncan Thomson, MITRE Corporation, March-April, 2004.

MITRE

Cisco CSA Agent CPU Overhead

CSA HIPS overhead appears to be in the range of 2%



* The performance indicator employed was the time to perform SNMP "MIB Walk" operations. Cisco tests were performed in 64-bit mode versus 32-bit mode for Sana. Data source: Duncan Thomson, MITRE Corporation, March-April, 2004.

MITRE

Network Traffic Measurements

- **Sana**
  - **"Heartbeat" only:** **1.5 Kbps background**
  - **Incident:** **10 to 20 Kbytes/alert**
- **CSA**
  - **Polling only:** **12.5 bits/second**
  - **Policy change:** **30 Kbytes**
  - **Incident:** **4.5 Kbytes/alert**

Sana Assessment

- Anomaly-based product required “training” in what was expected to be “normal” patterns
- Primary Response generated many false alerts (Type 1 errors)
  - The interactive, unstructured nature of the test application CRCT (Collaborative Routing Coordination Tools) contributed to this problem
- Sana also failed to catch a number of known Solaris exploits (Type II errors)
  - Vendor indicated that one of these failures was due to the fact that we were running an early version of Solaris 8
- MITRE concluded that Sana’s product was immature; not recommended for an FAA pilot implementation

CSA Assessment

- Like Sana's Primary Response, there are coverage issues, with CSA currently limited to Windows, Solaris and Linux
- CSA is extremely complex with literally hundreds of rule and configuration options
  - However, usable default configurations are provided
  - CAASD employed CSA defaults in its tests
- CSA passed all CAASD tests
- CAASD believes that CSA is worthy of being called a "Host-based Intrusion Prevention System" (HIPS)

Lessons Learned

- There is no substitute for direct lab experience with new security technologies
- Regarding the Internet-based evaluation, it may have been a more effective test with a Solaris "honey pot;" attackers did not have the skill—or adequate time—to break into a then-current patch level Solaris 8 environment and encounter the HIPS
- Scaling, monitoring, monitor integration, software maintenance and Microsoft—all pose issues that cloud the HIPS product category

The Prospect for 'Adaptive' Products

- At present there is a significant mismatch between the intelligence of the sophisticated attacker and the intelligence of the HIPS products
- The present products are off/on devices that must be "tuned" over time to generate the fewest possible Type I ("false positive") and Type II ("false negative") errors
- Any kind of change in the product settings, unless preceded by extensive testing, has the potential for initiating a self-imposed DoS

MITRE's Recommendations

- Conduct a long-term pilot (at least 6 months) with CSA on several different kinds of gateway servers (Solaris, Windows) in the administrative environment
  - Send several FAA operations staff to CSA training
- Keep careful records on Type I & II errors, server availability, and software maintenance requirements
- Re-evaluate the product—is it worth the additional expense and software maintenance?